UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

AVELARDO RIVERA and YASMINE ROMERO, individually and on behalf of all others similarly situated, Plaintiffs, v. AMAZON WEB SERVICES, INC., Defendant.	CASE NO. 2:22-cv-00269 ORDER

I

INTRODUCTION

This matter comes before the Court on Defendant Amazon Web Services, Inc.'s ("Amazon") motion to dismiss. Dkt. # 45. The Court has considered the submissions in support of, and in opposition to, the motion, the rest of the case file, and the applicable law. Being fully advised, the Court DENIES the motion.

II

BACKGROUND

"Biometrics" refers to technologies used to identify an individual based on unique physical characteristics. Dkt. # 88 at 3.[1] One of the most prevalent uses of biometrics is facial recognition technology, which works by scanning an image for a human face, extracting facial feature data, generating a "faceprint" through the use of facial recognition algorithms, and comparing the resultant faceprint to other faceprints stored in a faceprint database. *Id.* Amazon is one of many companies that have developed and produced facial recognition products. *Id.* at 5–11. Amazon's product, Rekognition, allows customers to add image and video facial recognition analysis to their applications, products, and services. *Id.* at 5. To do so, the customer must upload electronic images or videos to its Amazon cloud-storage accounts (also known as "S3 buckets") and then run a command within Rekognition called "index-faces" to extract biometric data from those images. *Id.* at 8. The customer can then use Rekognition to identify people within the images. *Id.* at 5–10. After the biometric data is extracted, it is stored in an Amazon back-end database called a Rekognition "collection." *Id.* at 8. One such customer that uses Rekognition is ProctorU Inc., a company that develops and licenses online test proctoring software for use by students and educational facilities. *Id.* at 10.

Plaintiffs Avelardo Rivera and Yasmine Romero are citizens and residents of Illinois who took multiple remote tests while attending two colleges in Illinois in 2019–2020. Dkt. # 88 at 2, 11. Both colleges used a proctoring software developed by ProctorU to administer the tests. *Id.* at 10–11. In order to identify Plaintiffs, the ProctorU software required them to submit their

[1] For the purposes of a motion to dismiss, the Court accepts all well-pleaded allegations in Plaintiffs' complaint as true and draws all reasonable inferences in favor of Plaintiffs. *See Wyler Summit P'ship v. Turner Broad. Sys., Inc.*, 135 F.3d 658, 661 (9th Cir. 1998).

images as well as images of valid identification documents. *Id.* at 11–12. Unbeknownst to Plaintiffs, the ProctorU software then used Amazon's Rekognition program to perform facial recognition on them and verify their identities. *Id.* Plaintiffs did not receive notice from Amazon, through ProctorU or otherwise, that Amazon was collecting, storing, or otherwise using their biometric data. *Id.* Plaintiffs were not asked for, nor did they provide, consent for Amazon to store, collect, or otherwise use their biometric data. *Id.* Plaintiffs allege that at no time while possessing their biometric data did Amazon maintain a publicly available retention and deletion schedule for biometric data. *Id.* They also allege that Amazon failed to destroy their biometric data after the initial purpose for collecting or maintaining their data had been satisfied. *Id.*

Plaintiffs bring a class action suit against Amazon for violating Illinois's Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), which regulates the collection, storage, and use of biometric identifiers and biometric information (collectively, "biometric data"). *See generally* Dkt. # 88. Specifically, Plaintiffs allege that Amazon violated section 15(a) and 15(b) of BIPA by possessing their biometric data without publishing or complying with a "retention schedule or guideline for permanently destroying Plaintiffs' and the Class's biometric data after the initial purpose for collecting or obtaining their biometric data had been satisfied," and by "collecting" the same data without providing adequate notice and obtaining their consent. *Id.* at 15–17.

Former lead plaintiff Jacinda Dorian filed her complaint in federal court on March 22, 2022. Dkt. # 1. Amazon filed its first motion to dismiss on May 16, 2022. Dkt. # 21. Amazon filed a motion to stay discovery on July 12, 2022, which the Court denied on August 8, 2022. Dkt. ## 29, 33. On August 30, 2022, Dorian moved to amend her complaint to substitute putative class members Avelardo Rivera ("Rivera") and Yasmine Romero ("Romero") in her place as the lead plaintiffs. Dkt. # 40. The Court granted the motion on September 20, 2022, and Plaintiffs Rivera and Romero filed an amended complaint on the same day. Dkt. ## 43, 44. Amazon moved to dismiss Plaintiffs' First Amended Complaint ("FAC") on October 19, 2022. Dkt. # 45. On July 17, 2023, the Court directed the parties to submit supplemental briefing regarding whether Plaintiffs have Article III standing to pursue their claims under Section 15(a) of BIPA. Dkt. # 79. On July 20, 2023, the parties filed a Stipulated Motion for Leave for Plaintiffs to File a Second Amended Complaint. Dkt. # 80. The Court granted the motion on July 21, 2023. Dkt. # 81. Plaintiffs filed their Second Amended Complaint ("SAC") on July 26, 2023. Dkt. # 88.

III

Discussion

When considering a motion to dismiss under Rule 12(b)(6), the Court construes the complaint in the light most favorable to the nonmoving party. *Livid Holdings Ltd. v. Salomon Smith Barney, Inc.*, 416 F.3d 940, 946 (9th Cir. 2005). The Court must accept all well-pleaded facts as true and draw all reasonable inferences in favor of the plaintiff. *Wyler Summit P'ship*, 135 F.3d at 661. The Court, however, is not required "to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 677–78. Dismissal under Rule 12(b)(6) can be based on the lack of a cognizable legal theory or the lack of sufficient facts alleged under a cognizable legal theory. *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988).

Amazon moves to dismiss all of Plaintiffs' claims in its instant motion. Dkt. # 45.

A. Article III Standing

As an initial matter, the Court is satisfied that Plaintiffs' SAC alleges sufficient facts to establish Article III standing on their Section 15(a) claim. Plaintiffs amended their complaint to allege that, in addition to failing to maintain a BIPA-compliant retention and deletion schedule, Amazon also failed to destroy Plaintiffs' data after the initial purpose for collecting or maintaining their data bad been satisfied. Dkt. # 88 at 11–12. The Seventh Circuit has held that such allegations establish Article III standing for a 15(a) claim. *See Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1149 (7th Cir. 2020) ("Fox alleges a concrete and particularized invasion of her privacy interest in her biometric data stemming from Dakkota's violation of the full panoply of its section 15(a) duties . . . [t]hese allegations suffice to plead an injury in fact for purposes of Article III."). Satisfied that Plaintiffs have established Article III standing, the Court turns to each of Amazon's arguments for dismissal.[2]

B. Definitions of "possess" and "collect"

Section 15(a) of BIPA applies only to private entities "in possession of" biometric data. 740 ILCS 14/15(a). Amazon argues that Plaintiffs' complaint does not allege facts showing that it "possessed" their data under 15(a). Dkt. # 45 at 12. Similarly, section 15(b) of BIPA is only triggered by those who "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data, and Amazon argues that Plaintiffs' complaint does not allege facts showing that Amazon did so. *Id.* at 17 (citing 740 ILCS 14/15(b)).

[2] The parties agree in their stipulated motion that, given the limited amendments in the SAC, the previous briefing on the motion to dismiss remains sufficient. Dkt. # 80 at 3. In the interest of resolving the motion as expeditiously as possible, the Court will not require the parties to re-file duplicative briefs.

i. Possession

BIPA does not define "possession." *See generally* 740 ILCS 14/1 *et seq*. The Court therefore "assumes the legislature intended for it to have it popularly understood meaning." *Rosenbach v. Six Flags Ent. Corp.,* 129 N.E.3d 1197, 1205 (Ill. 2019) (citations omitted). The Illinois Supreme Court has held that possession "occurs when a person has or takes control of the subject property or holds the property at his or her disposal." *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005). The *Ward* court elaborated that the legislature did not intend for the reader "to delve into the legal intricacies of the word 'possession,'" and noted the fact that possession does not require exclusive control over property. *Id.* at 561. Here, the Court similarly finds no indication that the ordinary meaning of possession does not apply.

Amazon's main argument is that, because it acted only as a back-end service provider, it did not even know of the presence of biometric data in ProctorU's S3 buckets, let alone exercise control over that data. Dkt. # 45 at 12–17. Instead, it states that only ProctorU "possessed" Plaintiffs' data within the meaning of BIPA. *Id.* at 14. Amazon cites several cases in which courts have dismissed Section 15(a) claims against customers acting only in a service provider capacity. *See Heard v. Becton, Dickinson & Co.,* 440 F. Supp. 3d 960, 962 (N.D. Ill. 2020) ("*Heard I*"); *Jacobs v. Hanwha Techwin Am., Inc.,* No. 21 C 866, 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021). Amazon also argues that Plaintiffs' reading of section 15(a) would invite absurd results because it would require Amazon to publish and comply with a retention and deletion schedule for data that it does not access or use. Dkt. # 45 at 15–17.

The Court is unpersuaded by Amazon's arguments. Plaintiffs have pleaded that, to use Amazon's Rekognition program, customers must "upload images to [Amazon]'s cloud-based storage solution." Dkt. # 88 at 8. They also allege after this upload occurs, Rekognition "accesses the relevant images and uses its machine vision algorithms to extract the facial geometry of individuals pictured . . ." *Id.* Lastly, Plaintiffs allege that the "feature vectors of facial geometry, as well as higher-order details such as whether a person is smiling, sad, or disgusted, or is wearing eyeglasses or sunglasses, are then stored in an [Amazon] backend database . . ." *Id.* The Court concludes that these allegations meet the common definition of the term "possession."

Courts have found possession to be sufficiently pleaded in analogous situations. For example, in a case from the Northern District of Illinois, a plaintiff sued the manufacturer of a medication dispensing system that required hospital workers to submit to a fingerprint scan to obtain medication for distribution to patients. *Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831, 836 (N.D. Ill. 2021) ("*Heard II*"). After the court first dismissed the plaintiff's complaint, he filed a First Amended Complaint clarifying that when a user enrolls in the medication dispensing system, the defendant stores their fingerprints on *both* the fingerprint devices *and* the defendant's servers. *Id.* at 840. The court found it significant that "the Pyxis system is not hermetically sealed within a hospital; users' biometric data flows back to BD's servers," and found that the allegations plausibly supported the conclusion that defendant was "in possession" of the users' biometric data. *Id.* Similarly, Plaintiffs here have pleaded that Amazon's program Rekognition "accesses" their biometric data to perform facial recognition, and then stores the same data on its back-end database, thereby making the data not hermetically sealed within the ProctorU program. *See* Dkt. # 88 at 8.

The cases Amazon cites to support its position are distinguishable. In *Heard I,* the court dismissed the plaintiff's complaint because it "merely parrot[ed] the statutory language" as to the defendant's alleged possession of the plaintiff's data. 440 F. Supp. 3d at 968. The court noted that, although the plaintiff claimed that the defendant "stored" his biometric information, this conclusory allegation did not allow the court to draw the reasonable inference that the defendant was "in possession" of his biometric data because the plaintiff did not explain whether the defendant exercised any form of control over the data, whether the defendant could access the data, or how the defendant allegedly received the data. *Id.* By contrast, here Plaintiffs specifically allege that Amazon receives their data when it is uploaded to their cloud-based storage. Dkt. # 88 at 8. Plaintiffs also allege that Amazon can access and control their data to perform facial recognition using its Rekognition program. *Id.* Plaintiffs have therefore supported their claim with substantially more factual allegations than the plaintiff in *Heard I.*

The other case cited by Amazon, *Jacobs,* involved a plaintiff who sued the manufacturer of security cameras installed at the entrance of a T.J. Maxx store in downtown Chicago. 2021 WL 3172967, at *1. In dismissing the plaintiff's complaint, the court noted that the plaintiff did "not allege that defendant installed the cameras, operated the cameras, or in any way accesse[d] or control[led] T.J. Maxx's security system," and that a full reading of the plaintiff's complaint suggested that "defendant's only alleged connection to those cameras was its role as the manufacturer and distributor." *Id.* at *2. In contrast, Plaintiffs here have alleged that Amazon did more than just create the Rekognition program and sell it to ProctorU; they allege that Amazon accessed their data during the facial recognition process and then stored their data on its back-end database. Dkt. # 88 at 8.

Lastly, the Court notes that Amazon's arguments about the practicality of creating and complying with a retention and deletion schedule are unconvincing, especially at the motion to dismiss phase, and arguably irrelevant to whether it has violated BIPA. As Judge Robart stated in *Vance-Amazon,* "there is nothing absurd about requiring any entity that obtains such information to comply with the safeguards that the Illinois legislature deemed necessary." *Vance v. Amazon.com Inc.*, 525 F. Supp. 3d 1301, 1313 (W.D. Wash. 2021); *see also Rosenbach,* 129 N.E.3d at 1207 ("[W]hatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers are information are not properly safeguarded; and the public welfare, security, and safety will be advanced. That is the point of the law.").

The Court concludes that Plaintiffs' SAC sufficiently supports the allegation that Amazon was "in possession" of their biometric data under section 15(a) of BIPA.

ii. Collection

BIPA does not define section 15(b)'s operative terms, which include "collect, capture, purchase, receive through trade, or otherwise obtain." 740 ILCS 14/15(b).[3] Amazon argues that collection requires something more than mere possession, and that "something more" is an affirmative act or active step. Dkt. # 45 at 17–18. To support this contention, Amazon cites the structure of the statute, which includes the term "possession" in section 15(a) but not 15(b), as well as several cases that distinguish between possession and collection. *See Heard I*, 440 F. Supp. 3d at 965–66; *Jacobs,* 2021 WL 31772967, at *2; *Namuwonge v. Kronos, Inc.,* 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019). Amazon argues that Plaintiffs' complaint does not allege that it took any "active step[s]" to collect their data. Dkt. # 45 at 18.

As an initial matter, it is unclear whether Amazon's interpretation of the statute is correct. At least one court has found that an entity may not "possess" biometric data without having first "collected" such data. *See Figueroa v. Kronos, Inc.,* 454 F. Supp. 3d 772, 783–84 (N.D. Ill. 2020). The *Kronos* court reasoned that Section 15(a) was likely intended to apply to entities that, before BIPA's effective date, already possessed biometric information, while Section 15(b) was intended to cover only those entities that came into possession of such information after BIPA's effective date. *Id.* But even assuming Amazon's reading is correct, Plaintiffs have alleged

[3] For simplicity's sake, the Court uses the word "collect" to encompass all the operative terms.

sufficient facts to support the inference that Amazon "collected" their data. Specifically, Plaintiffs allege that Amazon's program, Rekognition, "accesses" images after they have been uploaded, and "extract[s] the facial geometry of the individuals pictured into a feature vector." Dkt. # 88 at 8. Plaintiff also alleges that after this extraction of biometric data, Amazon stores the feature vectors on its own back-end database. *Id.*

Amazon again cites *Jacobs* to support its position, but as explained above, that case involved a defendant who merely manufactured and distributed security cameras to various T.J. Maxx stores. 2021 WL 3172967, at *3. Therefore, defendant's connection with the security cameras was essentially severed at the point of sale, and they were not involved in any data collection process that occurred once the cameras were installed. Conversely, here, Plaintiffs allege that Amazon continues to act as the "cloud-service provider" for ProctorU, and thus is able to "access" and "extract" biometric data that is uploaded to ProctorU's S3 buckets. Dkt. # 88 at 8–10. Amazon also cites *Namuwonge* and *Bernal,* two cases in which defendants provided plaintiffs' employers with timekeeping systems that recorded and stored employee fingerprints. *Namuwonge.,* 418 F. Supp. 3d at 286; *Bernal v. ADP, LLC,* No. 2017-CH-12364, 2019 WL 5028609, at *1 (Ill.Cir.Ct. Aug. 23, 2019). The courts dismissed plaintiffs' section 15(b) claims because they failed to allege any facts showing that the defendants collected, captured, or otherwise obtained their information. *Id.* But there, like in *Jacobs,* the plaintiffs did not allege any involvement in the data collection process on the part of defendants, beyond simply providing the technology to the plaintiffs' employers. Here, by contrast and as noted above, Plaintiffs allege that Amazon remains involved in the data collection process through Rekognition's "accessing" and "extraction" of biometric data and subsequent storage in their back-end database. Dkt. # 88 at 8–10.

This case is more analogous to *Heard II,* where the court stated:

> The FAC alleges that when a user enrolls in the Pyxis system, the device scans the user's fingerprint, extracts the unique features of that fingerprint to create a user template, and then stores users' biometric information both on the device and in [defendant's] servers. Data from subsequent scans are also stored on [defendant's] servers. These allegations suggest that [defendant] itself plays an active role in collecting or otherwise obtaining users' biometric information from the Pyxis devices.

Heard II, 524 F. Supp. 3d at 841. The defendant in *Heard II,* like in *Namuwonge* and *Bernal,* provided a technology to a third party, who then used the technology to collect and store plaintiffs' biometric data. But what allowed the complaint in *Heard II* to survive a motion to dismiss were the allegations that defendant continued to play an active role in "extract[ing]" and "stor[ing]" users' biometric data on their servers. The allegations here are quite similar to those in *Heard II,* and the Court therefore concludes that Plaintiffs have pleaded sufficient facts to support the inference that Amazon "collected" their data under Section 15(b).

Lastly, Amazon emphasizes the "absurd, inconvenient, [and] unjust consequences" that Plaintiffs' reading of BIPA would entail. Dkt. # 45 at 19 (citing *Solon v. Midwest Med. Records Ass'n., Inc.,* 925 N.E.2d 1113, 1118 (Ill. 2010)). In particular, Amazon contends that complying with BIPA's notice-and-consent requirement would be impracticable because Amazon "does not interact directly with ProctorU's end users or any of its customers' end users." *Id.* Amazon points to *Zellmer v. Facebook, Inc.,* a Northern District of California case in which the court rejected a BIPA claim brought by non-users of Facebook against Facebook, because it would be "patently unreasonable to construe BIPA to mean that" companies are "required to provide notice to, and obtain consent from," end users "who [are] for all practical purposes total strangers" to the companies. No. 18-cv-01880, 2022 WL 976981, at *3 (N.D. Cal. Mar. 31, 2022). But *Zellmer* is distinguishable because Plaintiffs are not "total strangers" to Amazon; rather, they are connected through ProctorU, and it is therefore not inconceivable that Amazon could notify them and obtain their consent during the image upload process. The Court therefore declines to dismiss Plaintiffs' complaint on these grounds.

C. Illinois Extraterritoriality Doctrine

In Illinois, statutes do not have extraterritorial effect "unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto Ins. Co.,* 835 N.E.2d 801, 852–53 (Ill. 2005). BIPA does not contain a provision suggesting that it is intended to apply extraterritorially. *See generally* 740 ILCS 14/1 *et seq.*; *see also Vance-Amazon,* 525 F. Supp. 3d at 1307. But the Ninth Circuit has stated, in the context of an appeal of class certification, that "it is reasonable to infer that the [Illinois] General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state." *Patel v. Facebook, Inc.,* 932 F.3d 1264, 1276 (9th Cir. 2019). To determine whether a law is being applied extraterritorially, the Illinois Supreme Court has instructed courts to consider whether the "circumstances relating to the transaction occur primarily and substantially" in Illinois. *Avery,* 835 N.E.2d at 853.

Amazon contends that it cannot be held liable under BIPA because Plaintiffs have not pleaded facts showing that Amazon "engaged in *any* conduct in Illinois, let alone that [Amazon]'s conduct occurred 'primarily and substantially' in Illinois." Dkt. # 45 at 21 (citing *Avery,* 216 Ill.2d at 187). Amazon analogizes Plaintiffs' claims to those in *McGoveran,* in which the District of Delaware dismissed BIPA claims against Amazon under the extraterritoriality doctrine. *McGoveran v. Amazon Web Servs., Inc.,* No. 20-cv-1399, 2021 WL 4502089, at *3 (D. Del. Sept. 30, 2021). There, the plaintiffs, all residents of Illinois, alleged that they called a third party's customer service representatives or call centers (located outside Illinois) from Illinois, and that the third party used an Amazon program to extract biometric data from the calls. *Id.* at *2. The court found that, at bottom, Plaintiff's allegations simply established that they were residents of Illinois, and that a "plaintiff's residency is not enough to establish an Illinois connection in order to survive a motion to dismiss based on extraterritoriality." *Id.* at *4. Amazon also cites *Vance v. Microsoft Corporation,* where Judge Robart granted summary judgment to Microsoft because discovery revealed that there was virtually no connection between the claims and Illinois other than the plaintiffs' residency. No. C20-1082-JLR, 2022 WL 9983979 (W.D. Wash. Oct. 17, 2022).

The Court concludes that the complaint in this case alleges facts beyond simply Plaintiffs' residency in Illinois. Plaintiffs also allege that they submitted their images and IDs through ProctorU while in Illinois, presumably from an Illinois-based Internet Protocol ("IP") address. *See* Dkt. # 88 at 8–10. Given the other allegations in the complaint, these facts could also support the inference that at least part of the data extraction process also occurred in Illinois. *Cf. In re Facebook Biometric Info Priv. Litig.,* 326 F.R.D. 535, 547 (N.D. Cal. 2018) ("[T]he functionality and reach of modern online services . . . cannot be compartmentalized into neat geographic boxes."). Further, although the *McGoveran* court rejected the plaintiffs' argument that any failure to provide BIPA-compliant notice and obtain BIPA-compliant consent "necessarily occurred in Illinois," *see McGoveran,* 2021 WL 4502089, at *4 ("it really makes no sense to assign a location for an act that did not occur."), other courts, including the Illinois Supreme Court, have found the location of purported failures or omissions to be relevant in analyzing extraterritoriality. *See, e.g.*, *Avery,* 835 N.E.2d at 854 ("The alleged deception in this case—the failure to disclose the inferiority of non-OEM parts—also occurred in Louisiana"); *Rivera v. Google Inc.,* 238 F. Supp. 3d 1088, 1101–02 (N.D. Ill. 2017) ("Rivera and Weiss also allege that it was in Illinois where Google failed to provide Rivera and Weiss with required disclosures and failed to get Rivera's and Weiss's consent"). Lastly, Plaintiffs' alleged injuries and those of the proposed class members occurred in Illinois. *See* Dkt. # 88 at 11–12.

The Court also notes that the inquiry of whether an alleged statutory violation occurs primarily and substantially within a state is "a highly fact-based analysis that is generally inappropriate for the motion to dismiss stage." *Vance v. Int'l Bus. Machs. Corp.,* No. 20 C 577, 2020 WL 5530134, at *3 (N.D. Ill. Sep. 15, 2020); *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *6 (N.D. Ill. 2017) (holding that the extraterritoriality doctrine is better addressed on a motion for summary judgment); *Rivera*, 238 F. Supp. 3d at 1101–02 (N.D. Ill. 2017) ("Discovery is needed to determine whether there are legitimate extraterritoriality concerns"); *Vance-Amazon,* 525 F. Supp. 3d at 1309 ("[M]ore discovery is needed to explore whether and to what extent Amazon's alleged acts . . . occurred in Illinois."). The Court thus finds Amazon's citation to Judge Robart's summary judgment order in *Vance-Microsoft* to be inapposite, since the court in that case had before it the full evidentiary record. Here, conversely, the Court does not have a full understanding of how Amazon's facial recognition technology operates, and therefore cannot say with certainty that Plaintiffs' suit would require extraterritorial application of BIPA. In light of these factors, the Court declines to dismiss Plaintiffs' complaint on extraterritoriality grounds.

D. Financial Institution Exemption

BIPA includes an exemption for "financial institutions." *See* 740 ILCS 14/25(c) ("Nothing in [BIPA] shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act ["GLBA"].").[4] Amazon argues that Plaintiffs' colleges are financial institutions under the

[4] Title V of the GLBA, 15 U.S.C. §§ 6801–6809, is a privacy law that regulates how financial institutions handle certain customer information. *See* 15 U.S.C. § 6801(a) (statement of policy); *see also Am. Bar Ass'n v. FTC*, 430 F.3d 457, 459 (D.C. Cir. 2005) (background). Under Title V, a "financial institution" is "any institution the business of which is engaging in financial activities," such as "[l]ending, exchanging, transferring, investing for others, or safeguarding money or securities"; "[p]roviding financial, investment, or economic advisory services"; and "[u]nderwriting, dealing in, or making a market in securities." 15 U.S.C. § 6809(3)(A); 12 U.S.C. § 1843(k)(4).

exemption, and that applying BIPA to Amazon would have the practical effect of applying BIPA to Plaintiffs' colleges, in violation of Section 25(c). *See* Dkt. # 45 at 25–27.

First, as Amazon acknowledges, the law is unclear on whether Plaintiffs' colleges do in fact qualify as "financial institutions" subject to the GLBA. *Compare Doe v. Northwestern Univ.*, 586 F. Supp. 3d 841, 841–42 (N.D. Ill. 2022) *and Duerr v. Bradley Univ.*, No. 21-CV-01096, 2022 WL 1487747, at *7 (C.D. Ill. Mar. 10, 2022) *with Patterson v. Respondus, Inc.*, Nos. 20 C 7692, 21 C 1785, 21 C 2620, 2022 WL 860946, at *21 (N.D. Ill. Mar. 23, 2022).[5] But even assuming they are, the Court cannot determine at this stage of briefing whether allowing Plaintiffs' claims to proceed would impermissibly apply BIPA's requirements to the colleges.[6] Amazon's contention is that requiring it to provide BIPA-compliant notice and obtain BIPA-compliant consent from ProctorU's end users would "necessarily interfere with the Colleges' [remote proctoring] activities, including by forcing the Colleges and ProctorU to redesign the interfaces" through which students sign in to take a test. Dkt. # 45 at 27. But the Court can imagine scenarios in which this would not be the case. For example, Amazon could create an alert displaying BIPA-compliant notice at the point of photo upload, *see* Dkt. # 88 at 10, and could instruct Rekognition not to run until it obtains the end user's BIPA-compliant consent.

[5] Amazon's argument that Plaintiffs' colleges are "financial institutions" under the 25(c) exemption relies on statements by the Consumer Financial Protection Bureau and the Federal Trade Commission. *See, e.g.*, 12 C.F.R. § 1016.1(b)(2)(ii); Fed. Trade Comm'n Privacy of Consumer Financial Information, 65 Fed. Reg. 33646, 33648 (May 24, 2000) (explaining that institutions of higher learning may qualify as financial institutions because many are significantly engaged in lending funds to consumers through financial aid programs). But at least one court has declined to follow this statement because it was not promulgated under the FTC's rulemaking authority. *See Patterson,* 2022 WL 860946, at *21–22, *22 n. 19. Further, the question of whether Plaintiffs' colleges are significantly engaged in lending funds to consumers could be a question of fact unsuitable for resolution on a motion to dismiss. *Id; see also Fee v. Illinois Inst. of Tech.*, No. 21-CV-02512, 2022 WL 2791818, at *5 (N.D. Ill. July 15, 2022).

[6] The Court notes that in all of Amazon's cited cases, the plaintiffs sued their schools directly, *see generally Northwestern Univ.,* 546 F. Supp. 3d 841; *Duerr,* 2022 WL 1487747, while here, Plaintiffs' schools are not parties to this action.

The Court does not see how providing such notice and obtaining such consent (or alternatively, requiring ProctorU to provide such notice and obtain such consent) before running Rekognition would "subject the Colleges' remote proctoring activities to all of BIPA's requirements," Dkt. # 45, as the colleges themselves would not have to publish their own retention and deletion schedule, would still be able to choose to use ProctorU for online examinations, and would not have to obtain their own notice and consent from students. In sum, without the benefit of additional evidence and briefing, the Court cannot resolve whether allowing Plaintiffs' claims to proceed would practically result in a violation of Section 25(c).

E. Definition of "aggrieved"

BIPA provides that "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." 740 ILCS 14/20. Amazon argues that Plaintiffs are not "aggrieved" parties because their legal rights have not been "adversely affected" or "invaded" by Amazon's conduct. Dkt. # 45 at 28 (citing *Rosenbach,* 129 N.E.3d at 1205). Amazon cites *Bryant v. Compass Grp. USA, Inc.* for the proposition that "the duty to disclose under section 15(a) is owed to the public generally, not to particular persons." 958 F.3d 617, 626 (7th Cir. 2020).

The Court concludes that Plaintiffs have alleged sufficient facts to show that they are "aggrieved" parties under the statute. First, the Court notes that *Bryant* is distinguishable because it involved a plaintiff who had alleged only a claim under the provision of 15(a) requiring *development* of a "written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information," not under the provision requiring *compliance* with the established retention schedule and destruction guidelines. *Bryant,* 958 F.3d at 626.[7] By contrast, here, Plaintiffs' SAC alleges not only that Amazon failed to maintain and publish a schedule and guidelines but also that it failed to destroy Plaintiffs' data after the initial purpose for collecting or maintaining their data bad been satisfied. Dkt. # 88 at 11–12. Plaintiffs have therefore alleged a more concrete and particularized injury than the plaintiff in Bryant.

Further, the Illinois Supreme Court has stated that, when a private entity fails to comply with Section 15's retention and destruction requirements, the violation constitutes an invasion of the privacy rights of the person whose data is subject to the breach. *See Rosenbach,* 129 N.E.3d at 1206. Although the plaintiff in *Rosenbach* alleged violations of Section 15(b), the court said this about BIPA in general:

> The duties imposed on private entities by section 15 of the Act regarding the collection, *retention*, disclosure, and *destruction* of a person's or customer's biometric identifiers or biometric information define the contours of that statutory right. Accordingly, when a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach … [S]uch a person or customer would clearly be "aggrieved" within the meaning of section 20 of the Act and entitled to seek recovery under that provision. No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action.

Id. (emphasis added). Plaintiffs here allege that Amazon violated its duties relating to retention and destruction of their biometric data. *See* Dkt. # 88 at 11–12. They have therefore alleged sufficient facts to make them "aggrieved" parties under the statute.

[7] The Court also acknowledges that in *Bryant,* the Seventh Circuit was tasked with deciding whether the plaintiff had Article III standing to pursue a 15(a) claim in federal court, not whether he was "aggrieved" within the meaning of the statute. But the Court agrees with Amazon that the case's holding is still relevant "to the nature and scope of the rights afforded under BIPA," (*see* Dkt. # 49 at 16 n. 8) because the two inquiries both focus on whether a plaintiff has alleged a concrete and individualized injury.

F. Amazon's Compliance with BIPA

Lastly, Amazon insists that—even if the Court concludes that it is subject to BIPA—it has done everything it possibly can to comply with the statute. Dkt. # 45 at 28–29. It explains that under its Service Terms, all Amazon customers who use Rekognition are required to provide legally adequate privacy notices and obtain necessary consent from end users. *Id.*

First, the Court notes that Amazon's Service Terms are not incorporated by reference in the SAC and were instead submitted by Amazon via a declaration, so it is unclear whether the Court can even consider them. *See Shaver v. Operating Engineers Loc. 428 Pension Tr. Fund*, 332 F.3d 1198, 1201 (9th Cir. 2003) ("Generally, on a 12(b)(6) motion, the District Court should consider only the pleadings") (citing *Lee v. City of Los Angeles,* 250 F.3d 668, 688–89 (9th Cir. 2001)). But even if it could, the Court is not convinced that Amazon's inclusion of a catch-all provision requiring its customers to comply with the law generally is enough to satisfy its legal obligations under BIPA. For example, as discussed above, Amazon could program Rekognition so that it will not run unless and until it provides BIPA-compliant notice and obtains BIPA-compliant consent from end users, either through ProctorU's interface or otherwise. *See supra,* Section D. To the extent that Amazon believes additional actions on its part would be "unfair and unreasonable" or "impossible to meet," *see* Dkt # 45 at 28 (citing *Midwest Bank & Tr. Co. v. Roderick,* 476 N.E.2d 1326, 1331–32 (Ill. App. 1985)), it may make those arguments at the summary judgment stage. But the face of Plaintiffs' complaint alleges sufficient facts to show that Amazon, a private entity, collected and maintained their data without complying with Section 15 of BIPA, thus surviving a motion to dismiss.

IV

Conclusion

For these reasons, the Court DENIES Amazon's motion to dismiss.

Dated this 26th day of July, 2023.

John H. Chun

John H. Chun
United States District Judge